New and changed information

This chapter describes the new and changed information in Cisco Unified Communications Manager (Cisco Unified CM) for Release 8.0(x).

For more information, refer to the latest release notes at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html.

- Cisco Unified Communications Manager release 8.5(1), page 1
- Cisco Unified Communications Manager release 8.0(2), page 13
- Cisco Unified Communications Manager release 8.0(1), page 15

Cisco Unified Communications Manager release 8.5(1)

This section describes the new and changed information in Cisco Unified Communications Manager, Release 8.5(1).

Alarm additions and changes

OPTIONS ping

Cisco Unified Communications Manager SIP OPTIONS allows a SIP trunk to track the status of remote destinations. The following new alarms are generated for OPTIONS ping:

- SIPTrunkISV
- SIPTrunkOOS
- SIPTrunkPartiallyISV

SIP Normalization and Transparency

Cisco Unified Communications Manager identifies the usage of and errors with SIP normalization scripts; that is, when the script gets opened and closed as well as when errors and resource warnings occur.

The following new alarms are generated for SIP Normalization and Transparency:

- SIPNormalizationScriptOpened

- SIPNormalizationScriptClosed
- SIPNormalizationResourceWarning
- SIPNormalizationScriptError
- SIPNormalizationAutoResetDisabled

Single Sign On and SmartCard Authentication (Chevette)

The parameters are modified for the following existing alarms:

- authLdapInactive
- authFail
- authSuccess

The following new alarms are generated for Single Sign On and SmartCard Authentication (Chevette):

- LDAPServerUnreachable
- SSODisabled
- SSONullTicket
- SSOServerUnreachable
- SSOUserNotInDB

Related Topics

Cisco Unified Serviceability alarms and CiscoLog messages

Enhanced reason codes for Device De-Reg

The following reason codes are added for EndPointTransientConnection alarms:

- maxDevRegExceeded—Maximum number of device registrations have been reached.
- DeviceInitiatedReset—Indicates that the error was due to device initiated reset.
- CallManagerReset—Indicates that the error was due to call manager reset.
- DirectoryNumberMismatch—Indicates mismatch between the directory number that the SIP device is trying to register with and the directory number configured in the Cisco Unified CM for the SIP device.
- DatabaseTimeout—Cisco Unified CM requested device configuration data from the database but did not receive a response within 10 minutes.
- RegistrationSequenceError—(SCCP only) A device requested configuration information from the Cisco Unified CM at an unexpected time. The Cisco Unified CM had not yet obtained the requested information. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be an internal firmware error.
- InvalidCapabilities—(SCCP only) The Cisco Unified CM detected an error in the media capabilities reported in the StationCapabilitiesRes message by the device during registration. The device will automatically attempt to register again. If this alarm occurs again, manually reset the device. If this alarm continues to occur after the manual reset, there may be a protocol error.

- CapabilityResponseTimeout—(SCCP only) The Cisco Unified CM timed out while waiting for the device to respond to a request to report its media capabilities. Possible causes include device power outage, network power outage, network configuration error, network delay, packet drops, and packet corruption. It is also possible to get this error if the Cisco Unified CM node is experiencing high CPU usage. Verify that the device is powered up and operating. Verify that network connectivity exists between the device and Cisco Unified CM, and verify that the CPU utilization is in the safe range.
- SecurityMismatch—Cisco Unified CM detected a mismatch in the security settings of the device and/or the Cisco Unified CM. The following mismatches are detected:
  - The device established a secure connection, yet reported that it does not have the ability to do authenticated signaling.
  - The device did not establish a secure connection, but the security mode configured for the device indicates that it should have done so.
  - The device established a secure connection, but the security mode configured for the device indicates that it should not have done so.
- autoRegisterDBError—Auto-registration of a device failed for one of the following reasons:
  - Auto-registration is not allowed for the device type.
  - An error occurred in the auto-registration stored procedure.
- DBAccessError—Device registration failed because of an error that occurred while building the station registration profile. This usually indicates a synchronization problem with the database.
- AutoRegisterDBConfigTimeout—(SCCP only) Cisco Unified CM timed out during auto-registration of a device. The registration profile of the device did not get inserted into the database in time. The device will automatically attempt to register again.
- DeviceTypeMismatch—The device type reported by the device does not match the device type configured on the Unified CM.
- AddressingModeMismatch—(SCCP only) Cisco Unified CM detected an error related to the addressing mode configured for the device. One of the following errors was detected:
  - The device is configured to use only IPv4 addressing, but did not specify an IPv4 address.
  - The device is configured to use only IPv6 addressing, but did not specify an IPv6 address.

The following reason codes are added for EndPointUnregistered alarms:

- NoEntryInDatabase—Device not configured properly in the Cisco Unified CM database.
- DatabaseConfigurationError—Device configuration error in the Cisco Unified CM database.
- DeviceNameUnresolveable—The Cisco Unified CM is unable to resolve the device name to an IP Address internally.
- MaxDevRegExceeded—Maximum number of device registrations have been reached.
- InitializationError—Indicates that an error occurred when the Cisco Unified CM tries to initialize the device.

- PowerSavePlus—The device powered off as a result of the Power Save Plus feature that is enabled for this device. When the device powers off, it remains unregistered from Cisco Unified CM until the Phone On Time defined in the Product Specific Configuration for this device.
- CallManagerForcedRestart—(SIP Only) The device did not respond to an Apply Config request and as a result, Unified CM sent a restart request to the device. The device may be offline due to a power outage or network problem. Confirm that the device is powered-up and that network connectivity exists between the device and Cisco Unified CM.
- SourceIPAddrChanged—(SIP Only) The device has been unregistered because the IP address in the Contact header of the REGISTER message has changed. The device will be automatically reregistered. No action is necessary.
- SourcePortChanged—(SIP Only) The device has been unregistered because the port number in the Contact header of the REGISTER message has changed. The device will be automatically re-registered. No action is necessary.
- RegistrationSequenceError—A device requested configuration information from the Unified CM at an unexpected time. The Unified CM no longer had the requested information in memory.
- InvalidCapabilities—(SCCP only) Cisco Unified CM detected an error in the updated media capabilities reported by the device. The device reported the capabilities in one of the StationUpdateCapabilities message variants.
- FallbackInitiated—The device has initiated a fallback and will automatically reregister to a higher-priority Cisco Unified CM. No action is necessary.
- DeviceSwitch—A second instance of an endpoint with the same device name has registered and assumed control. No action is necessary.

New Perfmon counters for Cisco SIP normalization

The Cisco SIP Normalization performance object contains counters that allow you to monitor aspects of the normalization script, including initialization errors, runtime errors, and script status. Each device that has an associated script causes a new instance of these counters to be created. The following table contains information on the Cisco SIP normalization counters.

Table 1: Cisco SIP normalization

Display Name	Description
DeviceResetAutomatically	This counter indicates the number of times that Cisco Unified CM automatically resets the device (SIP trunk). The device reset is based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration. When the device (SIP trunk) is reset due to script errors, the counter value increments. This count restarts when the device is reset manually.

Display Name	Description
DeviceResetManually	This counter indicates the number of times that the device (SIP trunk) is reset manually in Cisco Unified Communications Manager Administration or by other methods, such as AXL. When the device associated with a script is reset due to configuration changes, the counter value increments. The counter restarts in the following situations: • The SIP trunk is deleted. • The script on the trunk gets changed or deleted. • Cisco Unified Communications Manager restarts.
ErrorExecution	This counter represents the number of execution errors that occurred while the script executed. Execution errors can occur while a message handler executes. Execution errors can be caused by resource errors, an argument mismatch in a function call, and so on. When an execution error occurs, Cisco Unified CM performs the following actions: • Automatically restores the message to the original content before applying additional error handling actions. • Increments the value of the counter. • Takes appropriate action based on the configuration of the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in Cisco Unified Communications Manager Administration. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an execution error occurs. This counter provides a count from the most recent trunk reset that involved a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again.
ErrorInit	This counter represents the number of times a script error occurred after the script successfully loaded into memory, but failed to initialize in Cisco Unified CM. A script can fail to initialize due to resource errors, an argument mismatch in a function call, the expected table was not returned, and so on. Check the SIPNormalizationScriptError alarm for details, including the line number in the script that failed. Correct the script problem, upload the corrected script as needed, and reset the trunk. This counter increments every time an initialization error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone does not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment after you fix the script problem, examine the script again. When the error occurs during initialization, Cisco Unified CM automatically disables the script.

Display Name	Description
ErrorInternal	This counter indicates the number of internal errors that occurred while the script executed. Internal errors are very rare. If the value in this counter is higher than zero, a defect exists in the system that is not related to the script content or execution. Collect SDI traces and contact the Technical Assistance Center (TAC).
ErrorLoad	This counter represents the number of times a script error occurred when the script loaded into memory in Cisco Unified Communications Manager. A script can fail to load due to memory issues or syntax errors. Check the SIPNormalizationScriptError alarm for details. Check the script syntax for errors, upload the corrected script as needed, and reset the trunk. This counter increments every time a load error occurs. This counter provides a count from the most recent trunk reset that was accompanied by a script configuration change. (A device reset alone will not restart the count; the script configuration must also change before the reset occurs.) If the counter continues to increment even after you fix the script problem, examine the script again.
ErrorResource	This counter indicates whether the script encountered a resource error. Two kinds of resource errors exist: exceeding the value in the Memory Threshold field and exceeding the value in the Lua Instruction Threshold field. (Both fields display on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration.) If either condition occurs, Cisco Unified Communications Manager immediately closes the script and issues the SIPNormalizationScriptError alarm. If a resource error occurs while the script loads or initializes, the script is disabled. If a resource error occurs during execution, the configured system resource error recovery action is taken. (The setting of the System Resource Error Recovery Action field on the SIP Normalization Script Configuration window in Cisco Unified Communications Manager Administration defines this action.)
MemoryUsage	This counter specifies the amount of memory, in bytes, that the script consumes. This counter increases and decreases to match the amount of memory that the script uses. This count gets cleared when the script closes (because a closed script does not consume memory) and restarts when the script opens (gets enabled). A high number in this counter indicates a resource problem. Check the MemoryUsagePercentage counter and the SIPNormalizationResourceWarning alarm, which occur when the resource consumption exceeds an internally set threshold.
MemoryUsagePercentage	This counter specifies the percentage of the total amount of memory that the script consumes. The value in this counter is derived by dividing the value in the MemoryUsage counter by the value in the Memory Threshold field (in the SIP Normalization Script Configuration window) and multiplying the result by 100 to arrive at a percentage. This counter increases and decreases in accordance with the MemoryUsage counter. This count gets cleared when the script closes (because closed scripts do not consume memory) and restarts when the script opens (gets enabled). When this counter reaches the internally controlled resource threshold, the SIPNormalizationResourceWarning alarm is issued.

Display Name	Description
MessageRollback	This counter indicates the number of times that the system automatically rolled back a message. The system rolls back the message by using the error handling that is specified in the Script Execution Error Recovery Action field in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. When an execution error occurs, Cisco Unified CM automatically restores the message to the original content before applying additional error handling actions. If error handling specifies Rollback only, no further action is taken beyond rolling back to the original message before the normalization attempt. For the other possible Script Execution Error Recovery Actions, message rollback always occurs first, followed by the specified action, such as disabling the script, resetting the script automatically, or resetting the trunk automatically.
msgAddContentBody	This counter represents the number of times that the script added a content body to the message. If you are using the msg:addContentBody API in the script, this counter increases each time that the msg:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeader	This counter represents the number of times that the script added a SIP header to the message. If you are using the msg:addHeader API in the script, this counter increases each time that the msg:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to a SIP header in the message. If you are using the msg:addHeaderUriParameter API in the script, this counter increases each time that the msg:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to a SIP header in the message. If you are using the msg:addHeaderValueParameter API in the script, this counter increases each time that the msg:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgApplyNumberMask	This counter represents the number of times that the script applied a number mask to a SIP header in the message. If you are using the msg:applyNumberMask API in the script, this counter increases each time that the msg:applyNumberMask API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgBlock	This counter represents the number of times that the script blocked a message. If you are using the msg:block API in the script, this counter increases each time that the msg:block API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Display Name	Description
msgConvertDiversionToHI	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgConvertHIToDiversion	This counter represents the number of times that the script converted Diversion headers into History-Info headers in the message. If you are using the msg:convertDiversionToHI API in the script, this counter increases each time that the msg:convertDiversionToHI API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgModifyHeader	This counter represents the number of times that the script modified a SIP header in the message. If you are using the msg:modifyHeader API in the script, this counter increases each time that the msg:modifyHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveContentBody	This counter represents the number of times that the script removed a content body from the message. If you are using the msg:removeContentBody API in the script, this counter increases each time that the msg:removeContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeader	This counter represents the number of times that the script removed a SIP header from the message. If you are using the msg:removeHeader API in the script, this counter increases each time that the msg:removeHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgRemoveHeaderValue	This counter represents the number of times that the script removed a SIP header value from the message. If you are using the msg:removeHeaderValue API in the script, this counter increases each time that the msg:removeHeaderValue API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetRequestUri	This counter represents the number of times that the script modified the request URI in the message. If you are using the msg:setRequestUri API in the script, this counter increases each time that the msg:setRequestUri API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetResponseCode	This counter represents the number of times that the script modified the response code and/or response phrase in the message. If you are using the msg:setResponseCode API in the script, this counter increases each time that the msg:setResponseCode API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
msgSetSdp	This counter represents the number of times that the script set the SDP in the message. If you are using the msg:setSdp API in the script, this counter increases each time that the msg:setSdp API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.

Display Name	Description
ptAddContentBody	This counter represents the number of times that the script added a content body to the PassThrough (pt) object. If you are using the pt:addContentBody API in the script, this counter increases each time that the pt:addContentBody API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeader	This counter represents the number of times that the script added a SIP header to the PassThrough (pt) object. If you are using the pt:addHeader API in the script, this counter increases each time that the pt:addHeader API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderUriParameter	This counter represents the number of times that the script added a SIP header URI parameter to the PassThrough (pt) object. If you are using the pt:addHeaderUriParameter API in the script, this counter increases each time that the pt:addHeaderUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddHeaderValueParameter	This counter represents the number of times that the script added a SIP header value parameter to the PassThrough (pt) object. If you are using the pt:addHeaderValueParameter API in the script, this counter increases each time that the pt:addHeaderValueParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ptAddRequestUriParameter	This counter represents the number of times that the script added a request URI parameter to the PassThrough (pt) object. If you are using the pt:addRequestUriParameter API in the script, this counter increases each time that the pt:addRequestUriParameter API executes successfully. If the counter behavior is not as expected, examine the script logic for errors.
ScriptActive	This counter indicates whether the script is currently active (running on the trunk). The following values display for the counter: • 0—Indicates that the script is closed (disabled). • 1—Indicates that the script is open and operational. To open the script that should be running on this trunk, perform the following actions: **1** Check for any alarms that might indicate why the script is not open. **2** Correct any errors. **3** Upload a new script if necessary. **4** Reset the trunk.

Display Name	Description
ScriptClosed	This counter indicates the number of times that Cisco Unified Communications Manager has closed the script. When the script is closed, it is not enabled on this device. Cisco Unified CM closes the script under one of the following conditions: • The device was reset manually. • The device was reset automatically (due to an error). • The device was deleted. This count restarts when the SIP trunk is reset after a change to the script configuration and when Cisco Unified CM restarts.
ScriptDisabledAutomatically	This counter indicates the number of times that the system automatically disabled the script. The values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration determine whether the script is disabled. The script also gets disabled as a result of script error conditions that are encountered during loading and initialization. This counter provides a count from the most recent manual device reset that involved a script configuration change (a device reset alone does not restart the count; the script must also have changed before the reset occurs). This counter increments every time Cisco Unified CM automatically disables a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for SIPNormalizationScriptError alarm and SIPNormalizationAutoResetDisabled alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

Display Name	Description
ScriptOpened	This counter indicates the number of times that the Cisco Unified CM attempted to open the script. For the a script to open, it must load into memory in Cisco Unified CM, initialize, and be operational. A number greater than one in this counter means that Cisco Unified CM has made more than one attempt to open the script on this SIP trunk, either for an expected reason or due to an error during loading or initialization. The error can occur due to execution errors or resource errors or invalid syntax in the script. Expect this counter to be greater than one if any of these counters increment: DeviceResetManually, DeviceResetAutomatically, or ScriptResetAutomatically. The DeviceResetManually counter increments when an expected event, such as a maintenance window on the SIP trunk, causes the script to close. If the number in this counter is high for an unexpected reason, perform the following actions: • Check for alarms, such as the SIPNormalizationScriptClosed, SIPNormalizationScriptError, or SIPNormalizationResourceWarning. • Check resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files. This count restarts when the SIP trunk resets after a script configuration change and when Cisco Unified CM restarts.
ScriptResetAutomatically	This counter indicates the number of times that the system automatically reset the script. The script resets based on the values that are specified in the Script Execution Error Recovery Action and System Resource Error Recovery Action fields in the SIP Normalization Script Configuration window in Cisco Unified CM Administration. This counter specifies a count of the number of automatic script resets after the last manual device reset; this counter increments every time the Cisco Unified CM automatically resets a script due to script errors. If the number in this counter is higher than expected, perform the following actions: • Check for a SIPNormalizationScriptError alarm. • Check for any resource-related alarms and counters in RTMT to determine whether a resource issue is occurring. • Check for any unexpected SIP normalization events in the SDI trace files.

SNMP MIBs

The following TEXTUAL-CONVENTIONs are updated for 8.5(1) release:

- CcmDevUnregCauseCode
- CcmDevRegFailCauseCode

Related Topics

Cisco Management Information Base

Supported servers

The following IBM Server Models are supported for this release:

- MCS-7815-I2-IPC1
- MCS-7816-I3-IPC1
- MCS-7816-I4-IPC1/CCX1
- MCS-7816-I5-IPC1/CCX1
- MCS-7825-I2-IPC1
- MCS-7825-I3-IPC1
- MCS-7825-I4-IPC1
- MCS-7825-I5-IPC1
- MCS-7828-I3-SS1
- MCS-7828-I4-SS1
- MCS-7828-I5-SS1
- MCS-7835-I2-IPC1
- MCS-7835-I2-IPC2
- MCS-7835-I3-IPC1
- MCS-7845-I2-IPC1
- MCS-7845-I2-IPC2
- MCS-7845-I3-IPC1

The following HP Server Models are supported for this release:

- MCS-7816-H3-IPC1
- MCS-7825-H2-IPC1
- MCS-7825-H3-IPC1
- MCS-7825-H4-IPC1
- MCS-7828-H3-IPC1
- MCS-7835-H2-IPC1
- MCS-7835-H2-IPC2
- DL380G6 (Single E5504 CPU)
- MCS-7845-H2-IPC1
- MCS-7845-H2-IPC2

- DL380G6 (Single E5540 CPU)

The following Cisco Unified Computing Systems are supported for this release:

- UCS B200 M1
- UCS C210 M1

Related Topics

Vendor-specific Management Information Base

Cisco Unified Communications Manager release 8.0(2)

This section describes the new and changed information in Cisco Unified Communications Manager, Release 8.0(2). It contains information on new performance objects, and alerts for both the Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine server.

The Cisco Unified Real-Time Monitoring Tool runs on both the Cisco Unified Communications Manager servers and the Cisco Intercompany Media Engine server to provide information about system and feature health.

You can install RTMT onto a client machine from only one product type—Unified Communication Manager or Cisco Intercompany Media Engine. Installing RTMT client from different product types on the same client machine is not supported.

For information on installing RTMT on a Cisco Unified Communications Manager server, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

For information on installing RTMT on a Cisco Intercompany Media Engine server, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

Cisco Unified Communications Manager server

Performance Objects

The following performance objects are available on the Cisco Unified Communications Manager server to support Cisco Intercompany Media Engine. For descriptions of the objects and related counters, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

- IME Client
- IME Client Instance

Alerts

The following alerts are available on the Cisco Unified Communications Manager server to support Cisco Intercompany Media Engine. For descriptions and default configuration settings, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

- IMEDistributedCacheInactive
- IMEOverQuota

- IMEQualityAlert
- InsufficientFallbackIdentifiers
- IMEServiceStatus
- InvalidCredentials
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed

Cisco Intercompany Media Engine server

Performance Objects

The following performance objects are available on the Cisco Intercompany Media Engine server to support the Cisco Intercompany Media Engine feature. For descriptions of the objects and related counters, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

- IME Configuration Manager
- IME Server
- IME Server System Performance

Alerts

The following alerts are available on the Cisco Intercompany Media Engine server to support the Cisco Intercompany Media Engine feature. For descriptions and default configuration settings, refer to the *Cisco Intercompany Media Engine Installation and Configuration Guide*.

- BannedFromNetwork
- IMEDistributedCacheCertificateExpiring
- IMEDistributedCacheFailure
- IMESdlLinkOutOfService
- InvalidCertificate
- InvalidCredentials
- MessageOfTheDay
- SWUpdateRequired
- TicketPasswordChanged
- ValidationsPendingExceeded
- CriticalAuditEventGenerated

Cisco Unified Communications Manager release 8.0(1)

This section describes the new and changed information in Cisco Unified Communications Manager, Release 8.0(1).

Cisco Unified Serviceability

This section contains information about alarm additions, changes, and alarm obsoletion for the Cisco Unified Communications Manager Release 8.0(1).

Alarm additions and changes

Audit Log Catalog

The following new Audit Log alarms are added:

Alarm Name	Description
AdministrativeEvent	Failed to write into the primary file path. Audit Event is generated by this application. Severity level is Informational.
CriticalEvent	Failed to write into the primary file path. Audit Event is generated by this application. Severity level is Informational.
SecurityEvent	Failed to write into the primary file path. Audit Event is generated by this application. Severity level is Informational.

EM Alarm Catalog

The following new EM alarms are added:

Alarm Name	Description
EMAppInitializationFailed	EM Application not started. Error occurred while starting application. Severity level is Error.
EMAppStarted	EM Application started successfully. Severity level is Informational.
EMAppStopped	EM Application started. Application is shutting down gracefully because of an unloaded from Tomcat. Severity level is Notice.

Alarm Name	Description
EMCCFailedInLocalCluster	EMCC login failure occurred due to one of the following conditions: • Devices are incompatible with EMCC. • Unable to retrieve remote cluster information. • EMCC is restricted by the local cluster. • EMCC is restricted by the local cluster.
EMCCFailedInRemoteCluster	There was an EMCC login failure at a remote Unified CM. EMCC login could fail due to the following reasons: • User does not exist in any of the configured remote cluster. • User is not enabled for EMCC. • No free EMCC base device. • EMCC access was prevented by remote cluster. • Untrusted certificate received from the remote end while trying to establish a connection.
EMCCUserLoggedIn	EMCC login was successful. Severity level is Informational(6).
EMCCUserLoggedOut	EMCC logout was successful. Severity level is Informational(6).
EMServiceConnectionError	EM Service not reachable. EM Service might be down in one or more nodes in the cluster. Severity level is Error.
NodeNotTrusted	Untrusted Node was contacted. Severity level is Error.
UserInputFailure	EMCC login failure due to invalid user input due to invalid user credentials or the credentials have expired. Severity level is Warning(4).

TVS Alarm Catalog

The following new TVS alarms are added:

Alarm Name	Description
ConfigThreadChangeNotifyServerSingleFailed	Failed to allocate resources to handle configuration change notification from database.
ConfigThreadReadConfigurationFailed	Failed to retrieve enterprise parameter values from database at TVS service startup.

Alarm Name	Description
DefaultDurationInCacheModified	Default value of a Certificate duration in cache is modified in the Service Parameter page.
ITLFileRegenerated	New ITL File has been generated.
RollBackToPre8.0Disabled	Roll Back to Pre 8.0 has been disabled in the Enterprise Parameter page.
SDIControlLayerFailed	Failed to update trace logging or alarm subsystem for new settings.
TVSCertificateRegenerated	TVS Server certificate has been regenerated.
TVSServerListenBindFailed	Fail to connect to the network port through which file requests are received.
TVSServerListenSetSockOptFailed	Failed to increase the size of the network buffer for receiving file requests.

Call Manager Catalog

The following new Call Manager alarms are added:

Alarm Name	Description
CMVersionMismatch	One or more Unified CM nodes in a cluster are running different Cisco CallManager versions.
ConflictingDataIE	A call has been rejected because the incoming PRI/BRI Setup message had an invalid IE.
DbInfoCorrupt	Database information returned is corrupt. Database configuration error was encountered.
DbInfoError	Error in the database information retrieved. Database configuration error was encountered.
DbInfoTimeout	Database Information request timed out. Timeout was encountered while trying to read database configuration.
DbInsertValidatedDIDFailure	The Insertion of an IME provided E.164 DID has failed. A failure occurred attempting to insert a Cisco Unified Active Link learned DID.
EndPointRegistered	This alarm occurs when a device is successfully registered with Cisco Unified Communications Manager.

Alarm Name	Description
EndPointResetInitiated	This alarm occurs when a device is reset via the Reset button in Cisco Unified CM Administration.
EndPointRestartInitiated	Device restart initiated or Apply Config initiated on the specified device.
EndPointTransientConnection	End point transient connection attempt.
EndPointUnregistered	An endpoint that has previously registered with Cisco Unified Communications Manager has unregistered.
FirewallMappingFailure	Firewall unreachable.
IMEQualityAlertEntry	IME call quality problem.
IMEQualityAlertExit	IME call quality problem cleared.
IMEDistributedCacheInactive	Inactive IME distributed cache.
IMEOverQuota	Each IME server has a fixed quota on the total number of DIDs it can write into the IME distributed cache.
InsufficientFallbackIdentifiers	Cannot allocate fallback identifier.
InvalidSubscription	A message has been received from an IME server that contains a subscription identifier that is not handled by this node.
RouteRemoved	Route is removed automatically.
InvalidCredentials	Credential Failure to IME server.
PublicationRunCompleted	Completion of publication of published DID patterns.
PublishFailed	Unified CM attempted to store a number into the IME distributed cache, but the attempt failed. This is typically due to a transient problem in the IME distributed cache.
PublishFailedOverQuota	Each IME server has a fixed quota on the total number of DIDs it can write into the IME distributed cache.
RejectedRoutes	Rejected route due to Untrusted status.
TCPSetupToIMEFailed	Connection Failure to IME server.
TLSConnectionToIMEFailed	TLS Failure to IME service.
New SAF and CCD Alarms	
LostConnectionToSAFForwarder	Connection to the SAF Forwarder has been lost.

Alarm Name	Description
SAFForwarderError	SAF Forwarder error response sent to Unified CM.
SAFUnknownService	Unified CM does not recognize the service ID in a publish revoke or withdraw message.
SAFPublishRevoke	A CLI command revoked the publish action for the specified service or subservice ID.
SAFResponderError	This is raised when SAF forwarder doesn't know the transaction ID within SAF response from this Cisco Unified CM.
DuplicateLearnedPattern	This alarm occurs when CCD requesting service received a duplicate Hosted DN.
CCDIPReachableTimeOut	CCD Requesting Service IP Reachable Duration times out.
CCDPSTNFailOverDurationTimeOut	The internal limit on PSTN failover has expired.
CCDPSTNFailOverDurationTimeOut	CCD has reached the maximum number of learned patterns allowed.
New Alarms in External Call Control	
ConnectionFailureToPDP	A connection request from Unified CM to the policy decision point (PDP) failed.
ConnectionToPDPInService	A connection was successfully established between Cisco Unified Communications Manager (Unified CM) and the policy decision point (PDP).
AwaitingResponseFromPDPTimeout	Cisco Unified Communication Manager timed out waiting for the routing response from the policy decision point.
ErrorParsingResponseFromPDP	Cisco Unified Communications Manager failed to parse one or multiple optional elements or attributes in the call routing response from the policy decision point.
ErrorParsingDirectiveFromPDP	Cisco Unified Communications Manager (Unified CM) failed to parse the call routing directive or the diversion destination in the call routing response from the policy decision point (PDP).
FailureResponseFromPDP	The policy decision point (PDP) returned a 4xx (client) or 5xx (server) status code in the HTTP response.
CallAttemptBlockedByPolicy	A call was attempted but blocked or rejected by the policy decision point (PDP).
FailedToFulfillDirectiveFromPDP	Cisco Unified Communications Manager cannot fulfill the call routing directive returned by the PDP.

Alarm Name	Description
DigitAnalysisTimeoutAwaitingResponse	Cisco Unified Communications Manager sent a routing request to the policy decision point but the request timed out without a response.

Changed Alarms in Call Manager Catalog

The following existing CallManager alarms are updated:

Alarm Names	Alarm Changes
AnnunciatorNoMoreResourcesAvailable	Severity changed from Error to Warning
BChannelISV	Severity changed from Informational to Notice.
BChannelOOS	Severity changed from Error to Critical.
BeginThrottlingCallListBLFSubscriptions	Severity level is Warning.
CMInitializationStateTime	Severity level is Informational.
CMOverallInitTimeExceeded	Severity changed from Error to Alert.
CMTotalInitializationStateTime	Severity level is Informational.
CallManagerFailure	Severity changed from Error to Critical; Enum Definitions are updated.
CallManagerOnline	Severity level is Notice.
CodeRedEntry	Severity changed from Error to Critical.
CodeYellowEntry	Severity changed from Error to Critical.
CodeYellowExit	Severity changed from Error to Notice.
ConferenceNoMoreResourcesAvailable	Changed severity level from Error to Warning.
ConnectionFailure	Severity level is Error (3).
DBLException	Severity changed from Error to Alert.
DChannelISV	Severity changed from Informational to Notice
DChannelOOS	Severity changed from Error to Critical.
DaTimeOut	Severity changed from Error to Warning.
DatabaseDefaultsRead	Severity changed from Notice to Informational.

Alarm Names	Alarm Changes
DeviceApplyConfigInitiated	Severity level is Informational.
DeviceCloseMaxEventsExceeded	Severity level is Error (3).
DeviceDnInformation	Severity level is Informational (6).
DeviceInitTimeout	Severity level is Error (3)
DevicePartiallyRegistered	Following information is updated: • Enum Definitions for performance monitor object type • Enum Definitions for DeviceType
DeviceRegistered	Following information is updated: • Enum Definitions for Performance Monitor ObjType • Enum Definitions for Device type • Enum Definitions for IPAddrAttributes • Enum Definitions for IPV6AddrAttributes
DeviceResetInitiated	• Enum Definitions for DeviceType are updated. • Parameters added: Product type [String]
DeviceRestartInitiated	• Enum Definitions for DeviceType are updated. • Parameters added: Product type [String]
DeviceTransientConnection	• Severity changed from Error to Warning. • Following information is updated: ◦ Enum Definitions for DeviceType ◦ Enum Definitions ◦ Enum Definitions for IPAddrAttributes ◦ Enum Definitions for IPV6AddrAttributes

Alarm Names	Alarm Changes
DeviceTypeMismatch	Following information is updated: • Enum Definitions for DBDeviceType • Enum Definitions for DeviceType
DeviceUnregistered	• Severity changed from Error to Warning. • Following information is updated: ◦ Enum Definitions for DeviceType ◦ Enum Definition ◦ Enum Definitions for IPAddrAttributes ◦ Enum Definitions for IPV6AddrAttributes
EndThrottlingCallListBLFSubscriptions	Severity changed from Warning to Informational.
H323Started	• Severity changed from Informational to Notice. • Following information is updated: ◦ Parameters ◦ Enum Definitions for DeviceType
H323Stopped	Following information is updated: • Parameters • Enum Definitions for DeviceType
ICTCallThrottlingEnd	Severity changed from Error to Notice.
ICTCallThrottlingStart	Severity level is Error (3).
MGCPGatewayGainedComm	Severity changed from Informational to Notice.
MaliciousCall	Severity changed from Informational to Warning.

Alarm Names	Alarm Changes
MaxCallDurationTimeout	• Severity changed from Informational to Notice. • Following parameters added: ◦ Originating Device name(String) ◦ Destination Device name(String) ◦ Call start time(UInt) ◦ Call stop time(UInt) ◦ Calling Party Number(String) ◦ Called Party Number(String)
MaxCallsReached	Severity changed from Error to Critical.
MaxHoldDurationTimeout	Following parameters added: • Originating Device Name(String) • Destination Device Name(String) • Hold start time(UInt) • Hold stop time(UInt) • Calling Party Number(String) • Called Party Number(String)
MediaResourceListExhausted	Enum Definitions for MediaResourceType is updated.
MohNoMoreResourcesAvailable	Severity changed from Error to Warning.
MtpNoMoreResourcesAvailable	• Severity changed from Error to Warning. • Media Resource List Name parameter added.
MultipleSIPTrunksToSamePeerAndLocalPort	Severity level is Error.
NoFeatureLicense	Severity changed from Error to Emergency.
NotEnoughChans	• Severity changed from Error to Warning. • Device Name(String) is the only parameter.
NumDevRegExceeded	Severity level is Error (3).
PktCapOnDeviceStarted	Severity level is Informational (6).

Alarm Names	Alarm Changes
PktCapOnDeviceStopped	Severity level is Informational (6).
PktCapServiceStarted	Severity level is Informational (6).
PktCapServiceStopped	Severity level is Informational (6).
RouteListExhausted	Severity level is Warning.
RsvpNoMoreResourcesAvailable	Media Resource List Name(String) parameter is added.
SDLLinkISV	Severity changed from Informational to Notice.
SDLLinkOOS	Severity changed from Error to Alert.
SIPLineRegistrationError	• Severity changed from Error to Warning. • Enum Definitions for DeviceType are updated. • Enum Reasons table is updated
SIPStarted	• Severity changed from Informational to Notice. • Enum Definitions for InTransportType and OutTransportType are updated
SIPStopped	Enum Definitions for InTransportType and OutTransportType are updated.
StationAlarm	Severity level is Informational (6).
StationConnectionError	• Reason Code[Enum] parameter added. • Enum Definitions for Reason Code table added.
StationEventAlert	Severity changed from Error to Warning.
StationTCPInitError	• Severity changed from Error to Critical. • Following parameters are removed: ◦ Error Number [String] ◦ ErrorCode [Int]
TimerThreadSlowed	Severity changed from Warning to Critical.

Alarm Names	Alarm Changes
UserUserPrecedenceAlarm	• Severity changed from Error to Warning. • Enum definitions updated.

CDRRep Alarm Catalog

The following existing CDRRep alarms are updated:

Alarm Name	Alarm Changes
CDRAgentSendFileFailed	Changed Data Collector Routing List element to Alert Manager.
CDRAgentSendFileFailureContinues	Severity level is Error (3).
CDRFileDeliveryFailed	Changed Data Collector Routing List element to Alert Manager.
CDRFileDeliveryFailureContinues	Severity level is Error (3).
CDRHWMExceeded	Changed Data Collector Routing List element to Alert Manager.
CDRMaximumDiskSpaceExceeded	Facility and sub-facility changed. Added Routing List and changed Data Collector to Alert Manager.

Certificate Monitor Alarm Catalog

The following new Certificate Monitor alarms are added:

Alarm Name	Description
CertValidLessthanADay	Certificate is about to expire in less than 24 hours or has expired.
CertValidfor7days	Alarm indicates that the certificate has expired or expires in less than seven days.
CertValidityOver30Days	Alarm indicates that the certificate expiry is approaching but the expiry date is more than 30 days.
CertValidLessThanMonth	Alarm indicates that the certificate will expire in 30 days or less.

CMI Alarm Catalog

The following new CMI alarms are added:

Alarm Name	Description
CMIException	Error while reading the database.
CMIServiceStatus	CMI service is running and working properly.
DBLException	Unable to connect to the database.
InvalidPortHandle	The handle for the opened serial port is invalid.
MemAllocFailed	CMI tried to allocate memory and failed.
ParityConfigurationError	The CMI service parameter, Parity, has an invalid configuration.
ReadingFileFailure	CMI failed to read SMDI messages from the serial port.
SMDICmdError	CMI receives an invalid incoming SMDI message.
SMDIMessageError	SMDI message contains invalid DN.
SerialPortGetStatusError	When CMI tries to get the status of serial port, the operating system returns an error.
SerialPortOpeningError	When CMI tries to open the serial port, the operating system returns an error.
SerialPortSetStatusError	When CMI tries to set the status of serial port, the operating system returns an error.
StopBitConfigurationError	The Cisco Messaging Interface service parameter, Stop Bits, has an invalid configuration.
ThreadKillingError	An error occurred when CMI tried to stop the CMI service.
UnknownException	Unknown error while connecting to database.
VMDNConfigurationError	The Voice Mail DN for CMI is invalid.
WritingFileFailure	CMI failed to write SMDI messages to the serial port.

CTI Manager Alarm Catalog

The following new CTI Manager alarms are added:

Alarm Name	Description
ApplicationConnectionDropped	Application has dropped the connection to CTIManager.

Alarm Name	Description
ApplicationConnectionError	CTIManager is unable to allow connections from Applications.
CtiDeviceClosed	Application closed a device.
CtiDeviceInService	Device is back in service.
CtiDeviceOpenFailure	Application is unable to open the device.
CtiDeviceOpened	Application opened a device.
CtiDeviceOutofService	Device is out of service.
CtiIncompatibleProtocolVersion	Incompatible protocol version.
CtiLineClosed	Application closed the line.
CtiLineInService	Line is back in service.
CtiLineOpenFailure	Application is unable to open the line.
CtiLineOpened	Application opened the line.
CtiLineOpened	Line is out of service.
CtiMaxConnectionReached	Maximum number of CTI connections has been reached, no new connection will be accepted unless an existing connection is closed.
CtiProviderCloseHeartbeatTimeout	CTI heartbeat timeout occurred causing CTIManager to close the application connection.
CtiProviderClosed	CTI application closed the provider. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the application.
CtiProviderOpenFailure	CTI application is unable to open the provider. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the application.
CtiProviderOpened	CTI Application opened the provider successfully. The IP address is shown in either IPv4 or IPv6 format depending on the IP addressing mode of the Application.
CtiQbeFailureResponse	The requested operation from the application could not be performed because of a normal or abnormal condition.
InvalidQBEMessage	QBE PDU from application is invalid.

Alarm Name	Description
MaxDevicesPerNodeExceeded	An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Node.
MaxDevicesPerProviderExceeded	An application has opened more devices than the limit set in the CTIManager service parameter, Maximum Devices Per Provider.
RedirectCallRequestFailed	CTIManager is unable to redirect a call.
UnableToRegisterwithCallManagerService	CTI cannot communicate with Cisco CallManager service to register supplementary service features.
UnableToSetorResetMWI	An error occurred when setting the message waiting indication (MWI) lamp.

DB Alarm Catalog

The following existing DB alarms are updated:

Alarm Name	Alarm Changes
ErrorChangeNotifyClientBlock	Changed severity level to Critical from Error.
ErrorReadingInstalledRPMS	Severity level is Error (3).
IDSEngineCritical	Changed severity level to Error from Critical.
IDSEngineDebug	Changed severity level to Informational from Debug.
IDSReplicationInformation	Severity level is Informational.

DRF Alarm Catalog

The following new DRF alarms are added:

- DRFBackupCompleted—DRF backup completed successfully.
- DRFLocalDeviceError—DRF unable to access local device.
- DRFNoBackupTaken—A valid backup of the current system was not found after an Upgrade, Migration, or Fresh Install.
- DRFRestoreCompleted—DRF restore completed successfully.

IMS Alarm Catalog

The following existing IMS alarms are updated:

Alarm Name	Alarm Changes
AdminPassword	Severity level is Informational.
authAdminLock	Severity level is Warning (4).
authExpired	Added Routing List element and updated the parameter list.
authFail	Changed severity level from Notice to Warning.
authHackLock	Updated the parameter list.
authInactiveLock	Updated the parameter list.
authLdapInactive	Severity level is Warning (4).
authMustChange	• Parameter list is updated. • Routing List element is added.
authSuccess	Severity level is Informational (6).
credFullUpdateFailure	Severity level is Informational (6).
credFullUpdateSuccess	Severity level is Informational (6).
credReadFailure	Changed severity level to Notice from Informational. Updated parameter list and added Routing List element.
credReadSuccess	Severity level is Informational (6).
credUpdateFailure	Severity level is Informational (6).
credUpdateSuccess	Severity level is Informational (6).

IpVms Alarm Catalog

The following new IpVms alarm is added:

- kANNAudioFileMissing—Announcement file not found. The annunciator was unable to access an announcement audio file. This may be caused by not uploading a custom announcement to each server in the cluster or a locale has not been installed on the server.

Changed Alarms in IpVms Alarm Catalog

The following existing IpVms alarms are updated:

Alarm Name	Alarm Changes
ANNDeviceRecoveryCreateFailed	Added Routing List elements and Parameters.
CFBDeviceRecoveryCreateFailed	Added Routing List elements and Parameters.
MOHDeviceRecoveryCreateFailed	Severity changed from Error to Warning.
MTPDeviceRecoveryCreateFailed	Changed severity level from Error to Warning and added existing Routing List elements and Parameters.
SoftwareLicenseNotValid	Severity changed from Error to Warning.
SoftwareLicenseValid	Severity—Informational.
kANNAudioCreateDirFailed	• Severity changed from Error to Warning. • Parameter list updated.
kANNAudioUndefinedAnnID	• Severity changed from Error to Warning. • Parameter list removed.
kANNAudioUndefinedLocale	• Severity changed from Error to Warning. • Parameter list is updated.
kANNDeviceRecordNotFound	Severity changed from Warning to Error.
kANNDeviceStartingDefaults	• Severity changed from Informational to Warning. • Parameter list added.
kANNICMPErrorNotification	Parameter list updated.
kCFBDeviceRecordNotFound	Severity changed from Informational to Error.
kCFBDeviceStartingDefaults	• Severity changed from Informational to Warning. • New parameters added: ◦ Parameter Name(String) ◦ Value Used(String)

Alarm Name	Alarm Changes
kCFBICMPErrorNotification	Following parameters are removed: Call ID [ULong] Party ID [ULong] IP Port [ULong]
kChangeNotifyServiceCreationFailed	• Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int) ◦ OS Error Description(String)
kChangeNotifyServiceGetEventFailed	• Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int ◦ OS Error Description(String)
kChangeNotifyServiceRestartFailed	• Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code(Int) ◦ OS Error Description(String)
kCreateAudioSourcesFailed	Following parameters added: • OS Error Code(Int) • OS Error Description(String)
kCreateControlFailed	Following parameters added: • OS Error Code(Int) • OS Error Description(String)
kDeviceDriverError	Severity changed from Error to Warning.
kDeviceMgrCreateFailed	Severity changed from Error to Warning.
kDeviceMgrExitEventCreationFailed	Severity changed from Error to Warning.
kDeviceMgrLockoutWithCallManager	Severity changed from Error to Informational.
kDeviceMgrMoreThan50SocketEvents	Severity changed from Informational to Notice.

Alarm Name	Alarm Changes
kDeviceMgrOpenReceiveFailedOutOfStreams	Severity changed from Error to warning.
kDeviceMgrRegisterKeepAliveResponseError	Severity changed from Error to Warning.
kDeviceMgrRegisterWithCallManager	Severity level is Informational (6).
kDeviceMgrRegisterWithCallManagerError	Severity changed from Error to Warning.
kDeviceMgrSocketDrvNotifyEvtCreateFailed	Severity changed from Error to Warning.
kDeviceMgrSocketDrvNotifyEvtCreateFailed	Severity changed to Warning from Error.
kDeviceMgrStartTransmissionOutOfStreams	Severity changed from Error to Warning.
kDeviceMgrThreadWaitFailed	• Severity changed from Error to Informational. • Following parameters added: ◦ OS Error Code [Int] ◦ OS Error Description [String]
kDeviceMgrThreadxFailed	• Severity changed from Error to Warning. • Following parameters added: ◦ OS Error Code[Int] ◦ OS Error Description [String]
kDeviceMgrUnregisterWithCallManager	Severity level is Informational (6).
kFixedInputCodecStreamFailed	• Severity changed from Error to Warning. • Following parameters removed: ◦ Audio Source ID [ULong] ◦ System error code [ULong]
kFixedInputCreateControlFailed	• Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed.
kFixedInputCreateSoundCardFailed	• Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed

Alarm Name	Alarm Changes
kFixedInputInitSoundCardFailed	• Severity changed from Error to Warning. • Following parameters are removed: ◦ Audio Source ID [ULong] ◦ System error code [ULong]
kFixedInputTranscoderFailed	• Severity changed from Error to Warning. • Following parameters are removed: ◦ Audio Source ID [ULong ◦ System error code [ULong]
kGetFileNameFailed	• Severity changed from Error to Warning. • Audio Source ID [ULong] parameter is removed.
kIPVMSDeviceDriverNotFound	This alarm is available in 8.0(1).
kIPVMSMgrEventCreationFailed	Severity changed from Error to Warning.
kIPVMSMgrThreadxFailed	Severity changed from Error to Warning.
kIPVMSMgrWrongDriverVersion	Following parameters are removed: • Found [ULong] • Need [ULong]
kIPVMSStarting	ProcessID [ULong] parameter is removed.
kIPVMSStopping	ProcessID [ULong] parameter is removed.
kIpVmsMgrNoLocalHostName	Severity level is Error (3).
kIpVmsMgrNoLocalNetworkIPAddr	Severity level is Error (3).
kIpVmsMgrThreadWaitFailed	Severity changed from Error to Warning.

Alarm Name	Alarm Changes
kMOHBadMulticastIP	Severity changed to Warning from Error. Following parameters are removed: • Audio Source ID [ULong] • Call/Conference ID [ULong] • Multicast IP Port [ULong]
kMOHDeviceRecordNotFound	Severity changed from Informational to Warning.
kMOHICMPErrorNotification	Following parameters are removed: • Call ID [ULong] Party ID [ULong] IP Port [ULong]
kMOHMgrCreateFailed	• Severity changed from Error to Warning. • OS Error Description(String) parameter is added.
kMOHMgrExitEventCreationFailed	Severity changed from Error to Warning.
kMOHMgrIsAudioSourceInUseThisIsNULL	Severity level is Informational (6).
kMOHMgrThreadWaitFailed	• Severity changed from Error to Informational. • OS Error Description(String) parameter is added.
kMOHMgrThreadxFailed	• Severity changed from Error to Warning. • OS Error Description(String) parameter is added
kMOHRewindStreamControlNull	• Severity changed from Error to Informational. • Audio Source ID [ULong] parameter is removed.
kMOHRewindStreamMediaPositionObjectNull	• Severity changed from Error to Informational. • Audio Source ID [ULong] parameter is removed.
kMOHTFTPGoRequestFailed	Following parameters added: Error Description [String] Source Path [String] Destination Path [String] OS Error Code [Int] OS Error Description [String]

Alarm Name	Alarm Changes
kMTPDeviceRecordNotFound	Severity changed from Informational to Warning.
kMTPDeviceStartingDefaults	MTP Run Flag(String) parameter is added.
kPWavMgrThreadxFailed	Severity level is Error (3).
kReadCfgIpTosMediaResourceToCmNotFound	Severity level is Informational (6).
kReadCfgMOHEnabledCodecsNotFound	Severity level is Informational (6).
kReadCfgUserLocaleEnterpriseSvcParm	Severity level is Error (3).
kRequestedANNStreamsFailed	Following parameters are removed: Requested streams [ULong] Allocated streams [ULong]
kRequestedCFBStreamsFailed	Severity changed from Error to Warning.
kRequestedMOHStreamsFailed	Severity changed from Error to Warning.
kRequestedMTPStreamsFailed	Severity changed from Error to Warning.

JavaApplications Alarm Catalog

The following new JavaApplications alarms are added:

- CiscoHardwareLicenseInvalid—Installation on invalid or obsolete hardware. Cannot upload license files.
- CiscoLicenseFileInvalid—License File is invalid.

Changed alarms in JavaApplications Alarm Catalog

The following existing JavaApplications Alarms are updated:

- IPMAFilteringDown—Severity level is Error (3).
- WDStopped—Severity changed from Alert to Warning.

Login Alarm Catalog

The following existing Login Alarm is updated:

- AuthenticationFailed—Severity Changed from Error to Warning.

LpmTct Alarm Catalog

The following existing Login Alarms are updated:

Alarm Name	Description
CoreDumpFileFound	Severity level is Critical.
LogCollectionJobLimitExceeded	Severity changed from Informational to Warning.
LogFileSearchStringFound	Severity level is Informational.
LogPartitionHighWaterMarkExceeded	Severity changed from Error to Critical.
LogPartitionLowWaterMarkExceeded	Severity changed from Error to Warning.
SparePartitionHighWaterMarkExceeded	Severity changed from Error to Warning. **Note** Spare Partition is not used for Intercompany Media Engine server. So this alert will not be triggered for Intercompany Media Engine
SparePartitionLowWaterMarkExceeded	Severity level is Error (3). **Note** Spare Partition is not used for Intercompany Media Engine server. So this alert will not be triggered for Intercompany Media Engine

RTMT Alarm Catalog

The following new RTMT alarms are added:

- RTMT_ALERT—A Real-Time Monitoring Tool (RTMT) process in the AMC service uses the alarm mechanism to facilitate delivery of RTMT alerts in the RTMT AlertCentral or through email.

SystemAccess Alarm Catalog

The following existing System Access Alarms are updated:

- TotalProcessesAndThreadsExceededThresholdEnd—Severity changed from Informational to Notice.

TFTP Alarm Catalog

The following existing TFTP Alarms are updated:

Alarm Name	Description
CNFFBuffWriteToFilefopenfailed	Severity changed from Informational to Error.
CNFFBuffWriteToFilefwritefailed	Severity changed from Informational to Error.
ConfigItAllBuildFilesFailed	Severity changed from Informational to Error.
ConfigItAllReadConfigurationFailed	Severity changed from Informational to Error.

Alarm Name	Description
ConfigThreadBuildFileFailed	Severity changed from Informational to Error.
ConfigThreadCNCMGrpBuildFileFailed	Severity changed from Informational to Error.
ConfigThreadCNGrpBuildFileFailed	Severity changed from Informational to Error.
ConfigThreadChangeNotifyServerInstanceFailed	Severity changed from Error to Alert.
ConfigThreadChangeNotifyServerSingleFailed	Severity changed from Error to Alert.
ConfigThreadChangeNotifyServerStartFailed	Severity changed from Error to Alert.
ConfigThreadReadConfigurationFailed	Severity changed from Informational to Error.
CreateThreadFailed	Severity changed from Error to Alert.
NoCallManagerFound	Severity changed from Error to Warning.
SDIControlLayerFailed	Severity changed from Critical to Alert.

For more information on alarms, see Vendor-specific Management Information Base.

Obsolete alarms

The following alarms are obsoleted in this release:

Call Manager Catalog

- ConferenceCreated
- ConferenceDeleted
- CtiCallAcceptTimeout
- CtiStaleCallHandle
- DatabaseAuditInfo_074
- DatabaseDeviceNoDirNum
- DatabaseInternalDataError_06e
- DatabaseInternalDataError_06f
- DatabaseInternalDataError_070
- DatabaseInternalDataError_071
- DatabaseInternalDataError_072
- DatabaseInternalDataError_073
- DatabaseInternalDataError_075

- DnTimeout
- GatewayAlarm
- H323AddressResolutionError
- H323CallFailureAlarm
- MWIParamMisMatch
- NoConnection
- OutOfDnForAutoRegistration
- PktCapDownloadFailed
- PktCapDownloadOK
- PktCapLoginFailed
- PktCapLoginOK
- Redirection
- SIP IPPortConflict
- ThrottlingSampleActivity
- TotalCodeYellowEntry

CertMonitor Alarm Catalog

- CertExpired
- CertExpiryApproaching
- CertExpiryDebug
- CertExpiryError

CMI Alarm Catalog

- CCMConnectionError
- CMIDebugAlarm
- CMIServiceStarted
- CMIServiceStopped
- COMException
- ConfigParaNotFound
- DisconnectionToCCM
- WSAStartupFailed

CTI Manager Alarm Catalog

- kCtiDeviceOpenFailAccessDenied

- kCtiDirectoryLoginFailure
- kCtiEnvProcDevListRegTimeout
- kCtiExistingCallNotifyArrayOverflow
- kCtiIllegalEnumHandle
- kCtiIllegalFilterSize
- kCtiIllegalQbeHeader
- kCtiInvalidQbeSizeAndOffsets
- kCtiLineCallInfoResArrayOverflow
- kCtiLineOpenFailAccessDenied
- kCtiMYTCPSendError
- kCtiMytcpErrSocketBroken
- kCtiNewCallNotifyArrayOverflow
- kCtiNullTcpHandle
- kCtiProviderOpenInvalidUserNameSize
- kCtiQbeLengthMisMatch
- kCtiQbeMessageTooLong
- kCtiSdlErrorvException
- kCtiSsRegisterManagerErr
- kCtiTcpInitError
- kCtiUnknownConnectionHandle

DB Alarm Catalog

- ErrorChangeNotifyReconcile

IpVms Alarm Catalog

- kANNAudioComException
- kANNAudioOpenFailed
- kANNAudioTftpFileMissing
- kANNAudioTftpMgrCreate
- kANNAudioTftpMgrStartFailed
- kANNAudioThreadException
- kANNAudioThreadWaitFailed
- kANNAudioThreadxFailed
- kANNAudioXmlLoadFailed

- kANNAudioXmlSyntax
- kAddIpVmsRenderFailed
- kCfgListComException
- kCfgListDblException
- kCfgListUnknownException
- kCreateGraphManagerFailed
- kDeviceMgrThreadException
- kDownloadMOHFileFailed
- kFixedInputAddAudioCaptureDeviceFailed
- kFixedInputAddG711AlawIpVmsRenderFailed
- kFixedInputAddG711UlawIpVmsRenderFailed
- kFixedInputAddG729IpVmsRenderFailed
- kFixedInputAddMOHEncoderFailed
- kFixedInputAddWideBandIpVmsRenderFailed
- kFixedInputAudioCapMOHEncoderConnFailed
- kFixedInputAudioCaptureCreateFailed
- kFixedInputClassEnumeratorCreateFailed
- kFixedInputCreateGraphManagerFailed
- kFixedInputFindAudioCaptureDeviceFailed
- kFixedInputGetEventNotificationFailed
- kFixedInputGetFileNameFailed
- kFixedInputGetG711AlawIpVmsRendInfFailed
- kFixedInputGetG711AlawIpVmsRenderFailed
- kFixedInputGetG711UlawIpVmsRendInfFailed
- kFixedInputGetG711UlawIpVmsRenderFailed
- kFixedInputGetG729IpVmsRendInfFailed
- kFixedInputGetG729IpVmsRenderFailed
- kFixedInputGetMOHEncoderFailed
- kFixedInputGetMediaControlFailed
- kFixedInputGetMediaPositionFailed
- kFixedInputGetWideBandIpVmsRendInfFailed
- kFixedInputGetWideBandIpVmsRenderFailed
- kFixedInputMOHEncG711AlawRenderConnFail

- kFixedInputMOHEncG711UlawRenderConnFail
- kFixedInputMOHEncG729RenderConnFailed
- kFixedInputMOHEncWidebandRenderConnFail
- kFixedInputSetNotifyWindowFailed
- kGetEventNotificationFailed
- kGetIpVmsRenderFailed
- kGetIpVmsRenderInterfaceFailed
- kGetMediaControlFailed
- kGetMediaPositionFailed
- kMOHFilterNotifyError
- kMOHMgrThreadCreateWindowExFailed
- kMOHPlayStreamControlNull
- kMOHPlayStreamMediaControlObjectNull
- kMOHThreadException
- kMTPICMPErrorNotification
- kPWavMgrExitEventCreateFailed
- kPWavMgrThreadException
- kReadCfgANNComException
- kReadCfgANNDblException
- kReadCfgANNListComException
- kReadCfgANNListDblException
- kReadCfgANNListUnknownException
- kReadCfgANNUnknownException
- kReadCfgCFBComException
- kReadCfgCFBDblException
- kReadCfgCFBListComException
- kReadCfgCFBListDblException
- kReadCfgCFBListUnknownException
- kReadCfgCFBUnknownException
- kReadCfgDblGetChgNotifyFailed
- kReadCfgDblGetNodeNameFailed
- kReadCfgEnterpriseComException
- kReadCfgEnterpriseDblException

- kReadCfgEnterpriseException
- kReadCfgEnterpriseUnknownException
- kReadCfgMOHAudioSourceComException
- kReadCfgMOHAudioSourceDblException
- kReadCfgMOHAudioSourceUnknownException
- kReadCfgMOHComException
- kReadCfgMOHDblException
- kReadCfgMOHListComException
- kReadCfgMOHListDblException
- kReadCfgMOHListUnknownException
- kReadCfgMOHServerComException
- kReadCfgMOHServerDblException
- kReadCfgMOHServerUnknownException
- kReadCfgMOHTFTIPAddressNotFound
- kReadCfgMOHUnknownException
- kReadCfgMTPComException
- kReadCfgMTPDblException
- kReadCfgMTPListComException
- kReadCfgMTPListDblException
- kReadCfgMTPListUnknownException
- kReadCfgMTPUnknownException
- kRenderFileFailed
- kSetNotifyWindowFailed

Test Alarm Catalog

- TestAlarmWindows

Cisco Unified Real-Time Monitoring Tool

This section contains information about new perfmon counters.

New Perfmon counters

New perfmon counters are added for the following objects:

Cisco CallManager External Call Control

This feature provides information about the counters that are added to support the External Call Control feature. The following table contains information about the External Call Control counters.

Table 2: Cisco CallManager External Call Control

Counters	Counter Description
Cisco CallManager Object	
ExternalCallControlEnabledCallsAttempted	This counter specifies the total number of calls to devices that have the External Call Control feature enabled. This is a cumulative count of all calls to intercept-enabled patterns or DNs since the last restart of the Cisco CallManager service.
ExternalCallControlEnabledCallsCompleted	This counter specifies the total number of calls that were connected to a device that had the External Call Control feature enabled. This is a cumulative count of all calls to intercept-enabled patterns or DNs since the last restart of the Cisco CallManager service.
ExternalCallControlEnabledFailureTreatmentApplied	This counter specifies the total number of calls that were cleared or routed based on failure treatments (such as Allow or Deny) that are defined in the External Call Control profile.
External Call Control Objects	
PDPServersTotal	This counter defines the total number of PDP servers in all External Call Control Profiles configured in Cisco Unified CM Administration. This counter increments when a new PDP server is added and decrements when a PDP server is removed.
PDPServersInService	This counter defines the total number of in-service (active) PDP servers.
PDPServersOutOfService	This counter defines the total number of times that PDP servers have transitioned from in-service to out-of-service. This is a cumulative count of out-of-service PDP servers since the last restart of the Cisco CallManager service.
ConnectionsActiveToPDPServer	This counter specifies the total number of connections that Cisco Unified Communications Manager has established (currently active) with PDP servers.
ConnectionsLostToPDPServer	This counter specifies the total number of times that active connections between Cisco Unified Communications Manager and the PDP servers were disconnected. This is a cumulative count since the last restart of the Cisco CallManager service.

Cisco CallManager SAF

The Cisco SAF Client object provides information about SAF counters that are specific to each node. The following table contains information about Cisco SAF Client object counters.

Table 3: Cisco CallManager SAF Client Object

Counters	Counter Description
SAFConnectionsSucceeded (range from 0 to 2)	Total number of SAF client connections currently active on this Unified CM node.
SAFFConnectionsFailed (range from 0 to 2)	Total number of SAF client connections that failed on the Unified CM node. A failed connection is a connection that did not register with the SAF Forwarder.

Note A Cisco Unified CM node restart causes a counter reset.

Cisco Extension Mobility

The Cisco Extension Mobility object provides information about the extension mobility application. The following table contains information about the newly added Cisco Extension Mobility counters.

Table 4: Cisco Extension Mobility Application

Counters	Counter Description
Total Number of EMCC Messages	This represents the total number of messages related to EMCC Requests that came from remote clusters.
Number of Remote Devices	This represents the total number of devices from other clusters that are currently using a EMCC Base Device (EMCC Logged in).
Number of Unknown Remote Users	This represents the total number of users who were not found in any of the remote cluster during inter-cluster extension mobility login.
Active Inter-cluster Sessions	This represents the total number of inter cluster Extension Mobility requests that are currently in progress.
Total Number of Remote Users	This represents the total number of users from other cluster who use a local device of this cluster and have logged into a remote cluster.
EMCC Check User Requests Handled	This represents the total number of EMCC check user requests that came from remote clusters.

Cisco Feature Control Policy

The Cisco Feature Control feature provides information about the two new counters for TFTP. The following table contains information about the newly added Cisco Feature Control Policy feature counters.

Table 5: Cisco Feature Control Policy

Counters	Counter Description
BuildFeaturePolicyCount	Indicates the number of built FCP files
FeaturePolicyChangeNotifications	Indicates the number of sent FCP change notifications

Cisco IME Server

The Cisco IME Server provides information about the Performance Object and Counters for IME.

The following contains the Performance Object for Cisco IME Server:

VAPStatus (range from 0 to 2)—This flag indicates the overall health of the connection to the IME servers for a particular IME service. If 1, it means that Unified CM has successfully established a connection to its primary and, if configured, backup servers for the IME service. 2 = Unhealthy.

0 = Unknown.

The following table contains the Performance Counters for Cisco IME Server. The following table contains information about the Performance Counters for Cisco IME Server. For more information, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Table 6: Cisco IME Server

Counters	Counter Description
PublishedRoutes	Total number of DIDs published successfully into the DHT across all IME services. It is a dynamic measurement, and as such, gives you an indication of your own provisioned usage in addition to a sense of how successful the system has been in storing them into the network.
RejectedRoutes	Number of learned routes which were rejected because the number or domain were blacklisted by the administrator. This provides an indication of the number of 'missed opportunities' - cases where a VoIP call could happen in the future, but will not due to the blocked validation.
LearnedRoutes	Total number of distinct phone numbers which have been learned by IME and are present as routes in Unified CM's routing tables. If this number grows too large, it may exceed the per-cluster limit, and require additional clusters for scale.
UniqueDomains	Number of unique domain names of peer enterprises discovered by IME. It is an indicator of overall usage of the system.

Counters	Counter Description
FailedB2BLinkSetups	Total number of call attempts for which a IME route was available, but which were set up through the PSTN due to a failure to connect to the target over the IP network.
B2BLinkCallsAttempted	Number of calls initiated by UCM through IME. This includes calls that are accepted, as well as busy, no-answer and failed calls. The metric is strictly on initiation.
B2BLinkCallsSetup	Number of IME calls successfully placed by Unified CM and answered by the remote party, resulting in an IP call.
FailedFallbackCalls	Total number of failed fallback attempts.
e164 DIDs Learned	Number of DIDs learned from the IME server.
B2BLinkCallsAccepted	Number of IME calls successfully received by UCM and answered by the called party, resulting in an IP call.
B2BLinkCallsReceived	Number of calls received by Unified CM through IME. This includes calls that are accepted, as well as busy, no-answer and failed calls. The metric is strictly on initiation.

Cisco Unified CDR Analysis and Reporting

The functionality of Call Detail Records (CDR) Analysis and Reporting (CAR) is primarily to generate reports on Unified CM users and system status with respect to call processing records that are loaded to CAR database. CAR also does some CAR database management activities. CAR automatically schedules required tasks to take place or you can manually perform the tasks by using the web interface.

New Cisco CAR DB alarms

New alarms for the CAR DB instance separation get added in this release. A new thread of [CARIDSAlarm] gets created in the existing CAR Scheduler Service to receive the IDS alarms. There are four new categories and alarms with information specific to the IDS based on the class IDs.

The following new alarms support the CAR database instance:

- CARIDSEngineDebug—Indicates debug events from CAR IDS database engine. This alarm provides low-level debugging information from CAR IDS database engine. System administrator can disregard this alarm. Severity level is Debug(7).
- CARIDSEngineInformation—No error has occurred but some routine event completed in CAR IDS database engine. Severity level is Informational(6).
- CARIDSEngineCritical—This alarm does not compromise data or prevent the use of the system but does required attention. Severity level is Critical(2).

- CARIDSEngineFailure—Combined alarm for emergency and error situations. Something unexpected occurred that might compromise data or access to data or cause CAR IDS to fail. Severity level is Error(3).

Note For any alarms with severity levels at or higher than Critical, an alert gets automatically generated.

For more information, see *Cisco Unified CDR Analysis and Reporting Guide*.

New CAR object and counters

The new CAR counters monitor the CAR database space and shared memory usage. The following CAR counters for the Cisco CAR DB object get supported:

- RootDBSpaceUsed—Percentage of Root DB space consumed. The root DB space gets used by the IDS system tables in the CAR IDS instance.
- CARDBSpaceUsed—Percentage of CAR DB space consumed. The CAR DB space gets used by the CAR database.
- CARTempDBSpaceUsed—Percentage of CAR temporary DB space consumed. The CAR temporary DB space gets used by temporary tables in the CAR IDS instance and used by CAR applications.
- FreeSharedMemory—Total free and shared memory expressed in kilobytes (KB). Shared memory gets used by the database system and all database applications in the CAR IDS instance.
- UsedSharedMemory—Total used and shared memory expressed in kilobytes (KB). Shared memory gets used by the database system and all database applications in the CAR IDS instance.

There are no performance counters that monitor the CAR IDS processes individually because the counters get automatically added for each new process. The counters get implemented with a new thread/job of the CAR IDS performance in the existing CAR Scheduler service by using Java API (JNI based statsUpdate()).

Hunt/CTI integration for CAR reporting

CAR supports hunt groups and contains the following new reports:

- Hunt pilot summary
- Hunt pilot detailed report

Hunt pilot summary

Only CAR administrators generate the Hunt Pilot Summary Report.The CDR Hunt Pilot Call Summary report displays the call details for the specified hunt pilot. This report displays an only an overview of the calls for the hunt pilots and hunt member information is not included. The CAR administrator can generate report for a maximum of five hunt pilot DNs.

Hunt pilot detailed report

Only CAR administrators generate the Hunt Pilot Detailed Call Report. This report displays call details for a hunt pilot number or a hunt member DN.

CAR and CDRM alarm interface

CAR and CDRM allow the alarm interface to raise alerts. The alarm interface can generate Syslog events, SNMP traps, and e-mail notifications by using RIS/Collector/Alert Manager. CAR allows the performance interface to poll serviceability counters and to be monitored in Cisco Unified Real Time Monitoring Tool.

System-wide call tracking End-to-End Call Trace

The End-to-End Call Trace feature facilitates tracing calls that traverse multiple Cisco voice products, such as Unified CM, Cisco IOS Gateways, and other products.

There are four new CDR fields added: CAR Loader, schema, CDR export, CDR search reports and migration.

Related Topics

End-to-End Call Trace

Cisco Unified Call Detail Records

This feature traces calls that traverse multiple Cisco voice products by using the call records collected from each platform generated for the same call.

End-to-End Call Trace

To support the End-to-End call trace, following new fields have been added in the CDR search reports:

- IncomingProtocolID
- IncomingProtocolCallRef
- OutgoingProtocolID
- OutgoingProtocolCallRef

Remote destination to number mapping and CDRs

For an outgoing call to mobile users, the called party information in the CDR gets recorded based on the “Log Mobile Number in CDR” service parameter. The default equals False. If the service parameter is False, the enterprise number of the mobile user gets recorded in the CDR as the called party number. If the service parameter equals True, the mobile number gets recorded in CDR as the called party number.

New CDR fields to support Call Control Discovery

New codes display for the call control discovery feature, as described in the following table. (For more information on call control discovery, see Cisco Unified CDR Guide.)

Table 7: Codes for Call Control Discovery

Value	Type	Description
464	Redirect Reason Code	Indicates that the call is redirected to a PSTN failover number
131	Call Termination Code	Call Control Discovery PSTN Failover (Cisco specific)
29	OnBehalfof Code	CCDRequestingService

New CDR fields to support External Call Control

The following table describes the new CDR fields for the external call control feature. Use this table in conjunction with the Routing Reason Values for External Call Control table, which describes the routing reason values that are specific to external call control. For more information on external call control, see Cisco Unified CDR Guide.

CAR supports the new fields from the loader, CDR export, and CDR search reports on display and migration.

Table 8: CDR fields for External Call Control

Field Name	Range of Values	Description
currentRoutingReason	Positive Integer	This field, which is used with the external call control feature, displays the reason why the call was intercepted for the current call. For a list of reasons, see the Routing Reason Values for External Call Control table. Default value is 0.
origRoutingReason	Positive Integer	This field, which is used with the external call control feature, displays the reason why the call was intercepted for the first time. For a list of reasons, see the Routing Reason Values for External Call Control table. Default value is 0.
lastRedirectingRoutingReason	Positive Integer	This field, which is used with the external call control feature, displays why the call was intercepted for the last time. For a list of reasons, see the Routing Reason Values for External Call Control table. Default - Empty string.

The following table includes the reasons that can display for the currentRoutingReason, origRoutingReason, or lastRedirectingRoutingReason fields.

Table 9: Routing reason values for External Call Control

Value that Displays in the Field	Reason	Description
0	PDPDecision_NONE	This value indicates that the route server did not return a routing directive to the Cisco Unified Communications Manager.
1	PDPDecision_Allow_Fulfilled	This value indicates that Cisco Unified Communications Manager allowed a call.
2	PDPDecision_Allow_Unfulfilled	This value indicates that Cisco Unified Communications Manager disallowed a call.
3	PDPDecision_Divert_Fulfilled	This value indicates that Cisco Unified Communications Manager diverted the call.
4	PDPDecision_Divert_Unfulfilled	This value indicates that Cisco Unified Communications Manager was not able to divert the call.
5	PDPDecision_Forward_Fulfilled	This value indicates that Cisco Unified Communications Manager forwarded the call.
6	PDPDecision_Forward_Unfulfilled	This value indicates that Cisco Unified Communications Manager was unable to forward the call.
7	PDPDecision_Reject_Fulfilled	This value indicates that Cisco Unified Communications Manager rejected the call.
8	PDPDecision_Reject_Unfulfilled	This value indicates that Cisco Unified Communications Manager was not able to reject the call.

New CDR support for iSAC Codec

The codec fields can now support the iSAC (Media_Payload_ISAC) with the value of 89.

New CDR fields for hunt list support

The following table describes the new CDRs for the hunt list support (see Cisco Unified CDR Guide for more information).

Table 10: CDR fields for Hunt Lists

Field Name	Range of Values	Description
huntPilotDN	Text String	This field indicates the hunt pilot DN through which the call is routed. Default - Empty string.
huntPilotPartition	Text String	This field indicates the partition for the hunt pilot DN. Default - Empty string.
huntPilotDN	Text String	This field indicates the hunt pilot DN through which the call is routed. Default - Empty string.

Cisco Unified Reporting

There are no updates for Cisco Unified Reporting Guide in the Release 8.0(1).

MIB updates for 8.0(1)

The following table lists the deprecated and replaced MIBs.

Table 11: Updated MIBs

Action	Description
Deprecated	CcmDevFailCauseCode; Added CcmDevRegFailCauseCode and CcmDevUnregCauseCode
Deprecated	ccmPhoneStatusReason; Added ccmPhoneUnregReason and ccmPhoneRegFailReason in ccmPhoneTable
Deprecated	ccmPhoneFailCauseCode; Added ccmPhoneFailedRegFailReason in ccmPhoneFailedTable
Deprecated	ccmPhoneStatusUpdateReason; Added ccmPhoneStatusUnregReason and ccmPhoneStatusRegFailReason in ccmPhoneStatusUpdateTable

Action	Description
Deprecated	ccmGatewayStatusReason; Added ccmGatewayUnregReason and ccmGatewayRegFailReason in ccmGatewayTable.
Deprecated	ccmMediaDeviceStatusReason; Added ccmMediaDeviceUnregReason and ccmMediaDeviceRegFailReason in ccmMediaDeviceTable.
Deprecated	ccmCTIDeviceStatusReason; Added ccmCTIDeviceUnregReason and ccmCTIDeviceRegFailReason in ccmCTIDeviceTable
Deprecated	ccmH323DevStatusReason; Added ccmH323DevUnregReason and ccmH323DevRegFailReason in ccmH323DeviceTable.
Deprecated	ccmVMailDevStatusReason; Added ccmVMailDevUnregReason and ccmVMailDevRegFailReason in ccmVoiceMailDeviceTable.
Deprecated	ccmGatewayFailCauseCode; Added ccmGatewayRegFailCauseCode in ccmNotificationsInfo.
Deprecated the following Notification Type	ccmGatewayFailed and added ccmGatewayFailedReason.
Deprecated following OBJECT_GROUPS	ccmPhoneInfoGroupRev5, ccmNotificationsInfoGroupRev4, ccmGatewayInfoGroupRev3, ccmMediaDeviceInfoGroupRev3, ccmCTIDeviceInfoGroupRev3, ccmH323DeviceInfoGroupRev2, ccmVoiceMailDeviceInfoGroupRev1 and ccmNotificationsGroupRev2; Added following OBJECT_GROUPS: ccmPhoneInfoGroupRev6, ccmNotificationsInfoGroupRev5, ccmGatewayInfoGroupRev4, ccmMediaDeviceInfoGroupRev4, ccmCTIDeviceInfoGroupRev4, ccmH323DeviceInfoGroupRev3, ccmVoiceMailDeviceInfoGroupRev2, ccmNotificationsGroupRev3.

Action	Description
Deprecated following MODULE-COMPLIANCE	ciscoCcmMIBComplianceRev6; Added ciscoCcmMIBComplianceRev7.
Obsoleted following OBJECT_GROUPS	ccmInfoGroupRev3, ccmH323DeviceInfoGroupRev1